US-CERT National Cyber Alert System

SB04-266-Summary of Security Items from September 15 through September 20, 2004

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans identified between September 13 and September 20, 2004. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Bugs, Holes, & Patches

- Windows Operating Systems
  - Google Toolbar Input Validation
  - IBM OEM Microsoft Windows Default Administrative Account
  - McAfee VirusScan Arbitrary Code Execution
  - Microsoft Windows CE KDatastruct Information Disclosure
  - Microsoft Windows XP Explorer.EXE TIFF Image Denial of Service
  - Microsoft Internet Explorer User Security Confirmation Bypass
  - **Microsoft JPEG Processing Buffer Overflow (Updated)**
  - Rhinosoft DNS4Me Denial Of Service & Cross-Site Scripting Vulnerabilities
  - Snitz Forums 'Down.ASP' Input Validation
  - Tech-Noel Pigeon Server Remote Denial of Service
  - Virtual Programming VP-ASP 'shoprestoreorder.asp' Remote Denial of Service
- UNIX / Linux Operating Systems
  - **Apache mod_ssl Denial of Service (Updated)**
  - **Apache mod_ssl Remote Denial of Service (Updated)**
  - Apple iChat Remote Link Application Execution
  - **Apple QuickTime Streaming Server Remote Denial of Service (Updated)**
  - **wvWare Buffer Overflow Vulnerability (Updated)**
  - **GNU a2ps Command Injection (Updated)**
  - GNU Radius SNMP String Remote Denial of Service
  - **GNU Aspell Stack Buffer Overflow (Updated)**
  - **CDRTools Unspecified Privilege Escalation (Updated)**
  - **Star Tape Archiver Superuser Access (Updated)**
  - **Webmin / Usermin Insecure Temporary File (Updated)**
  - LOGICNOW PerlDesk 'lang' Parameter Input Validation
  - MacOSXLabs RsyncX Local Vulnerabilities
  - **Kerberos 5 krb5_aname_to_localname' Multiple Buffer Overflows (Updated)**
  - Mozilla Firefox Default Installation File Permission
  - **mpg123 'do_layer2() Function' Remote Buffer Overflow (Updated)**
  - Multiple Vendors Apache mod_dav Remote Denial of Service
  - Multiple Vendors Apache Web Server Remote IPv6 Buffer Overflow
  - Multiple Vendors Apache Web Server Configuration File Buffer Overflow
  - **Multiple Vendors Kerberos 5 Double-Free Vulnerabilities (Updated)**
  - **Multiple Vendors MIT Kerberos 5 ASN.1 Decoder Remote Denial of Service (Updated)**
  - Multiple Vendors CUPS Browsing Denial of Service
  - **Multiple Vendors MLib/IMLib2 Multiple BMP Image (Updated)**
  - **Multiple Vendors KDE Konqueror Cookie Domain Validation (Updated)**
  - Multiple Vendors gdk-pixbug BMP, ICO, and XPM Image Processing Errors
  - Multiple Vendors LinuxPrinting.org Foomatic-Filter Arbitrary Code Execution
  - **Multiple Vendors TNFTPD Multiple Signal Handler Remote Privilege Escalation (Updated)**
  - Multiple Vendors LibXpm Image Decoding Multiple Remote Buffer Overflow
  - Multiple Vendors Samba-VScan Remote Denial of Service
  - **OpenOffice/StarOffice Insure Temporary File Permissions (Updated)**
  - SUS Format String
  - **PHP 'memory_limit' and strip_tags() Remote Vulnerabilities (Updated)**
  - **Samba Remote Print Change Notify Remote Denial of Service (Updated)**
  - **Samba Remote Denials of Service (Updated)**
  - SnipSnap HTTP Response Splitting
  - **SpamAssassin Remote Denial of Service (Updated)**
  - **Squid Proxy NTLM Authentication Remote Denial of Service (Updated)**
  - Sudo Information Disclosure
  - vBulletin SQL Injection
  - Xine-lib Multiple Buffer Overflows
- Multiple Operating Systems
  - Business Objects WebIntelligence Access Control Bypass & Cross-Site Scripting
  - HP Web Jetadmin Unspecified Arbitrary Command Execution
  - Inkra 1504GX Remote Denial of Service
  - Matt Smith ReMOSitory SQL Injection
  - Mozilla Multiple Vulnerabilities
  - Multiple Browser Cookie Domain Validation
  - **Multiple Vendors NSS Buffer Overflow (Updated)**
  - MyServer Directory Traversal
  - PHP Group PHPP 'phpinfo()' Function Information Disclosure
  - PHPGroupWare Cross-Site Scripting
  - SMC7004VWBR & SMC7008ABR Authentication Bypass
  - YaBB Administrator Command Execution & Cross-Site Scripting
  - ZyXEL P681 ARP Request Information Disclosure

Recent Exploit Scripts/Techniques

Trends

Viruses/Trojans

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Google Toolbar 1.1.41-1.1.49, 1.1.53-1.1.60, 2.0.114.1	An input validation vulnerability exists in the 'About' section of the Google Toolbar due to insufficient filtering of HTML code, which could let a remote malicious user execute arbitrary HTML and JavaScript code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Google Toolbar Input Validation	High	Bugtraq, September 17, 2004
IBM Microsoft Windows XP SP1 OEM Version, Microsoft Windows XP OEM Version	A vulnerability exists due to a default hidden administrative account that fails to set a password, which could let a malicious user obtain administrative access. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	IBM OEM Microsoft Windows Default Administrative Account	High	SECNAP Advisory, September 15, 2004
McAfee VirusScan 4.5, 4.5.1	A vulnerability exists in 'System Scan' via the system tray applet due to the failure to drop privileges, which could let a malicious user execute arbitrary code. This issue has reportedly been addressed by the vendor in Patch 48, which may be obtained by customers with a valid contract grant number through McAfee Corporate Technical Support. There is no exploit code required.	McAfee VirusScan Arbitrary Code Execution	High	iDEFENSE Security Advisory, September 15, 2004
Microsoft Windows CE 2.0, 3.0, 4.2	A vulnerability exists in the kernel memory structure KDataStruct, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. This vulnerability is exploited by the virus WinCE.Duts.A.	Microsoft Windows CE KDatastruct Information Disclosure	Medium	Airscanner Mobile Security Advisory, September 18, 2004
Microsoft Windows XP Home SP1 Microsoft Windows XP Home Microsoft Windows XP Professional SP1 Microsoft Windows XP Professional	A Denial of Service vulnerability exists in 'Explorer.exe' due to the way certain TIFF format images are handled, No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Windows XP Explorer.EXE TIFF Image Denial of Service	Low	SecurityFocus, September 16, 2004
Microsoft Internet Explorer 6.0 SP2	A vulnerability exists due to a design error, which could let a malicious user bypass the user confirmation requirement. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Microsoft Internet Explorer User Security Confirmation Bypass	Medium	Bugtraq, September 15, 2004
Microsoft Microsoft .NET Framework 1.x, Digital Image Pro 7.x, 9.x, Digital Image Suite 9.x, Frontpage 2002, Greetings 2002, Internet Explorer 6, Office 2003 Professional Edition, 2003 Small Business Edition, 2003 Standard Edition, 2003 Student and Teacher Edition, Office XP, Outlook 2002, 2003, Picture It! 2002, 7.x, 9.x, PowerPoint 2002, Producer for Microsoft Office PowerPoint 2003, Project 2002, 2003, Publisher 2002, Visio 2002, 2003, Visual Studio .NET 2002, 2003, Word 2002; **Avaya DefinityOne Media Servers, IP600 Media Servers, S3400 Modular**	A buffer overflow vulnerability exists in the processing of JPEG image formats, which could let a remote malicious user execute arbitrary code. Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx **Proofs of Concept exploit scripts have been published**	Microsoft JPEG Processing Buffer Overflow CVE Name: CAN-2004-0200	High	Microsoft Security Bulletin, MS04-028, September 14, 2004 US-CERT Vulnerability Note VU#297462, September 14, 2004 **Technical Cyber Security Alert TA04-260A, September 16, 2004**

Messaging, S8100 Media Servers				**SecurityFocus, September 17, 2004**
RhinoSoft.com DNS4Me 3.0 .0.4	Two vulnerabilities exist: a Denial of Service vulnerability exists due to an error when processing incoming traffic; and a Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published for the Cross-Site Scripting vulnerability.	DNS4Me Denial Of Service & Cross-Site Scripting Vulnerabilities	Low/High (High if arbitrary code can be executed)	GulfTech Security Research Advisory, September 16, 2004
Snitz Forums 2000 Snitz Forums 2000 3.0, 3.1, 3.3 .03, 3.3 .02, 3.3 .01, 3.3, 3.4 .04, 3.4.03, 3.4 .02	A vulnerability exists in the 'down.asp' script due to insufficient sanitization of the 'location' parameter, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Snitz Forums 'Down.ASP' Input Validation	High	Securiteam, September 19, 2004
Tech-Noel Inc. Pigeon Server 3.2.143	A remote Denial of Service vulnerability exists when a malicious user submits a login parameter value longer than 8180 characters to port 3103. Upgrade available at: ftp://ftp.tech-noel.com/PigeonServerUpd.exe There is no exploit code required.	Pigeon Server Remote Denial of Service	Low	Securiteam, September 19, 2004
Virtual Programming VP-ASP 5.0	A remote Denial of Service vulnerability exists because a malicious user can restore a previous order using 'shoprestoreorder.asp.' Fix available at: http://www.vpasp.com/virtprog/info/faq_securityfixes.htm We are not aware of any exploits for this vulnerability.	VP-ASP 'shoprestoreorder.asp' Remote Denial of Service	Low	SecurityTracker Alert ID, 1011359, September 19, 2004

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Apache Software Foundation Apache 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.50	A remote Denial of Service vulnerability exists in Apache 2 mod_ssl during SSL connections. Apache: http://nagoya.apache.org/bugzilla/show_bug.cgi?id=29964 RedHat:http://rhn.redhat.com/errata/RHSA-2004-349.html SuSE: ftp://ftp.suse.com/pub/suse/i386/update/ **Gentoo: http://security.gentoo.org/glsa/glsa-200409-21.xml** **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **Trustix: http://http.trustix.org/pub/trustix/updates/** We are not aware of any exploits for this vulnerability.	Apache mod_ssl Denial of Service CVE Name: CAN-2004-0748	Low	SecurityFocus, September 6, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:096, September 15, 2004** **Gentoo Linux Security Advisory, GLSA 200409-21, September 16, 2004** **Trustix Secure Linux Security Advisory,TSLSA-2004-0047, September 16, 2004**
Apache Software Foundation Apache 2.0.50	A remote Denial of Service vulnerability exists in 'char_buffer_read()' when using a RewriteRule to reverse proxy SSL connections. Patch available at: http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_io.c?r1=1.125&r2=1.126 SuSE: ftp://ftp.suse.com/pub/suse/ **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **RedHat: http://rhn.redhat.com/errata/RHSA-2004-463.html** **Gentoo: http://security.gentoo.org/glsa/glsa-200409-21.xml** **Trustix: http://www.trustix.org/errata/2004/0047/** There is no exploit code required; however, Proofs of Concept exploits have been published.	Apache mod_ssl Remote Denial of Service CVE Name: CAN-2004-0751	Low	SecurityTracker Alert ID, 1011213, September 10, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:096, September 15, 2004** **RedHat Security Advisory, RHSA-2004:463-09, September 15, 2004** **Gentoo Linux Security Advisory GLSA 200409-21, September 16, 2004** **Trustix Secure Linux Security Advisory , TSLSA-2004-0047, September 16, 2004**

Apple iChat 1.0.1, AV 2.0, 2.1	A vulnerability exists when a remote malicious iChat user submits a specially crafted 'link' that, when activated by the target user, will cause an application on the target user's system to run. Patches available at: http://www.apple.com/support/downloads/ There is no exploit code required.	iChat Remote Link Application Execution CVE Name: CAN-2004-0873	High	Apple Security Advisory, APPLE-SA-2004-09-16, September 17, 2004
Apple Mac OS X 10.2.8, 10.3.4, 10.3.5	A remote Denial of Service vulnerability exists in the QuickTime Streaming Server when a malicious user submits a particular sequence of operations. Security update available at: http://www.apple.com/support/downloads/ We are not aware of any exploits for this vulnerability.	Apple QuickTime Streaming Server Remote Denial of Service CVE Name: CAN-2004-0825	Low	APPLE-SA-0024-09-07 Security Update, September 7, 2004 **US-CERT Vulnerability Note VU#914870, September 15, 2004**
Caolan McNamara and Dom Lachowicz wvWare version 0.7.4, 0.7.5, 0.7.6 and 1.0.0	A buffer overflow vulnerability exists due to the insecure function call strcat() without appropriate bounds checking, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.abisource.com/bonsai/cvsview2.cgi?diff_mode=context&whitespace_mode=show&root=/cvsroot&subdir=wv&command=DIFF_FRAMESET&root=/cvsroot&file=field.c&rev1=1.19&rev2=1.20 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200407-11.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ **Debian: http://security.debian.org/pool/updates/main/w/wv/** A Proof of Concept exploit has been published.	wvWare Library Buffer Overflow Vulnerability CVE Name: CAN-2004-0645	High	Securiteam, July 11, 2004 iDEFENSE Security Advisory, July 9, 2004 Conectiva Linux Security Announcement, CLA-2004:863, September 10, 2004 **Debian Security Advisory, DSA 550-1, September 20, 2004**
GNU a2ps 4.13	A vulnerability exists in filenames due to insufficient validation of shell escape characters, which could let a malicious user execute arbitrary commands. FreeBSD: http://www.freebsd.org/cgi/cvsweb.cgi/~checkout~/ports/print/a2ps-letter/files/patch-select.c?rev=1.1&content-type=text/plain **SuSE: ftp://ftp.suse.com/pub/suse/** There is no exploit code required; however, a Proof of Concept exploit has been published.	GNU a2ps Command Injection	High	Securiteam, August 29, 2004 **SUSE Security Announcement, SUSE-SA:2004:034, September 17, 2004**
GNU Radius 0.92.1, 0.93-0.96, 1.1, 1.2	A remote Denial of Service vulnerability exists in the 'asn_decode_string()' function in 'snmplib/asn1.c' when a malicious user submits a large unsigned integer in the SNMP parameter. Update available at:ftp://alpha.gnu.org/gnu/radius/ We are not aware of any exploits for this vulnerability.	GNU Radius SNMP String Remote Denial of Service CVE Name: CAN-2004-0849	Low	iDEFENSE Security Advisory, September 15, 2004
GNU Gentoo Aspell 0.50.5; Gentoo Linux 1.4	A buffer overflow vulnerability exists in the 'word-list-compress' utility due to insufficient bounds checking, which could let a malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200406-14.xml **OpenPKG: ftp://ftp.openpkg.org/** Proofs of Concept exploits have been published.	GNU Aspell Stack Buffer Overflow CVE Name: CAN-2004-0548	High	Securiteam, June 14, 2004 Gentoo Linux Security Advisory, GLSA 200406-14, June 17, 2004 **OpenPKG Security Advisory, OpenPKG-SA-2004.042, September 15, 2004**
J. Schilling CDRTools 2.0, 2.0.1 a18, 2.0.3.	A vulnerability exists in 'cdrecord,' which could let a malicious user obtain root privileges. **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Gentoo: http://security.gentoo.org/glsa/glsa-200409-18.xml** **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/** Exploit scripts have been published.	CDRTools Unspecified Privilege Escalation CVE Name: CAN-2004-0806	High	SecurityFocus, August 31, 2004 **US-CERT Vulnerability Note VU#700326, September 17, 2004**
J.Schilling Star Tape Archiver 1.5a09-1.5a45	A vulnerability exists in the setuid function due to a failure to properly implement the function when ssh is used for remote tape access, which could let a malicious user obtain superuser access. Update available at: http://ftp.berlios.de/pub/schily/star/alpha/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-11.xml We are not aware of any exploits for this vulnerability.	Star Tape Archiver Superuser Access CVE Name: CAN-2004-0850	High	SecurityTracker Alert ID: 1011195, September 8, 2004 **US-CERT Vulnerability Note VU#339089, September 17, 2004**
Jamie Cameron	A vulnerability exists due to the insecure creation of temporary files during installation, which	Webmin /	Medium	SecurityFocus,

Usermin 1.0 80, 1.0 70, 1.0 60, 1.0 51, 1.0 40, 1.0 30, 1.0 20, 1.0 10, 1.0 00, Webmin1.0 90, 1.0 80, 1.0 70, 1.0 60, 1.0 50, 1.0 20, 1.0 00, 1.100, 1.110, 1.121, 1.130, 1.140, 1.150	could let a malicious user obtain sensitive information. Usermin: http://freshmeat.net/redir/usermin/28573/url_tgz/usermin-1.090.tar.gz Webmin: http://prdownloads.sourceforge.net/webadmin/webmin-1.160.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200409-15.xml **Debian: http://security.debian.org/pool/updates/main/w/webmin/** There is no exploit code required.	Usermin Insecure Temporary File CVE Name: CAN-2004-0559		September 10, 2004 **Debian Security Advisory, DSA 544-1, September 14, 2004**
LOGICNOW PerlDesk	A vulnerability exists in the 'pdesk.cgi' software due to insufficient validation of the 'lang' parameter, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploit has been published.	PerlDesk 'lang' Parameter Input Validation	Medium	SecurityTracker Alert ID, 1011276, September 15, 2004
MacOSXLabs RsyncX 2.1	Two vulnerabilities exist: a vulnerability exists due to a failure to drop 'wheel' group privileges, which could let a malicious user execute arbitrary programs; and a vulnerability exists in '/tmp/cron_rsyncxtmp' because the temporary file is created insecurely, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	RsyncX Local Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1011352, September 17, 2004
MIT Debian Fedora Gentoo Immunix Mandrake OpenBSD RedHat SGI Sun Tinysofa Trustix Kerberos 5 1.0, 1.0.6, 1.0.8, 1.1, 1.1.1, 1.2.1-1.2.7, 1.3 -alpha1, 5.0 -1.3.3, 5.0 -1.2beta1&2, 5.0 -1.1.1, 5.0 -1.1, 5.0 -1.0.x; tinysofa enterprise server 1.0 -U1, 1.0	Multiple buffer overflow vulnerabilities exist due to boundary errors in the 'krb5_aname_to_localname()' library function during conversion of Kerberos principal names into local account names, which could let a remote malicious user execute arbitrary code with root privileges. Patch available at: http://web.mit.edu/kerberos/advisories/2004-001-an_to_ln_patch.txt Mandrake: http://www.mandrakesoft.com/security/advisories Tinysofa: http://www.tinysofa.org/support/errata/2004/009.html Trustix: http://http.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/k/krb5/ Fedora: http://securityfocus.com/advisories/6817 RedHat: http://rhn.redhat.com/errata/RHSA-2004-236.html SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ Sun: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57580 Gentoo: http://security.gentoo.org/glsa/glsa-200406-21.xml Apple: http://www.apple.com/support/downloads/ **Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000860** Currently we are not aware of any exploits for this vulnerability.	Kerberos 5 'krb5_aname_to_localname' Multiple Buffer Overflows CVE Name: CAN-2004-0523	High	MIT krb5 Security Advisory 2004-001, June 3, 2004 TA04-147A, http://www.kb.cert.org/vuls/id/686862tp Apple Security Update, APPLE-SA-2004-09-07, September 7, 2004 **Conectiva Security Advisory, CLSA-2004:860, September 10, 2004**
Mozilla.org Mozilla Browser 1.7, rc3, 1.7.1, 1.7.2; Firefox 0.9 rc, 0.9-0.9.3	A vulnerability exists due to improper file permissions, which could let a remote malicious user execute arbitrary code. Firefox http://www.mozilla.org/products/firefox/releases/0.10.html Mozilla Browser: http://www.mozilla.org/releases/ There is no exploit code required.	Mozilla Firefox Default Installation File Permission	High	Bugtraq, September 13, 2004 US-CERT Vulnerability Note VU#653160, September 17, 2004
mpg123.de mpg123 0.x	A buffer overflow vulnerability exists in the 'do_layer2()' function, which could let a remote malicious user execute arbitrary code. **Gentoo: http://security.gentoo.org/glsa/glsa-200409-20.xml** We are not aware of any exploits for this vulnerability.	mpg123 'do_layer2() Function' Remote Buffer Overflow	High	Securiteam, September 7, 2004 **Gentoo Linux Security Advisory, GLSA 200409-20, September 16, 2004**

Multiple Vendors
Apache Software Foundation Apache 2.0.50 & prior; Gentoo Linux 1.4;
RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3;
Trustix Secure Enterprise Linux 2.0,
	A remote Denial of Service vulnerability exists in the Apache mod_dav module when an authorized malicious user submits a specific sequence of LOCK requests.
	Update available at: http://httpd.apache.org/
	Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200409-21.xml
	RedHat: ftp://updates.redhat.com/enterprise
	Trustix: ftp://ftp.trustix.org/pub/trustix/updates/
		Apache mod_dav Remote Denial of Service
		CVE Name:
		CAN-2004-0809
			Low	SecurityTracker Alert ID, 1011248, September 14, 2004

Secure Linux 2.0, 2.1	There is no exploit code required; however, Proof of Concept exploit has been published.			
Multiple Vendors Apache Software Foundation Apache 2.0.50 & prior; Gentoo Linux 1.4; MandrakeSoft Linux Mandrake 9.2, amd64, 10.0, AMD64; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3, Fedora Core1&2; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1; Turbolinux Turbolinux Desktop 10.0	A buffer overflow vulnerability exists in the apr-util library's IPv6 URI parsing functionality due to insufficient validation, which could let a remote malicious user execute arbitrary code. *Note: On Linux based Unix variants this issue can only be exploited to trigger a Denial of Service condition.* Patch available at: http://www.apache.org/dist/httpd/patches/apply_to_2.0.50/CAN-2004-0747.patch Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200409-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Redhat: http://rhn.redhat.com/errata/RHSA-2004-463.html http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SuSE: ftp://ftp.suse.com/pub/suse Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates We are not aware of any exploits for this vulnerability.	Apache Web Server Remote IPv6 Buffer Overflow CVE Name: CAN-2004-0786	Low/High (High if arbitrary code can be executed)	SecurityFocus, September 16, 2004
Multiple Vendors Apache Software Foundation Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.50; Gentoo Linux 1.4; MandrakeSoft Linux Mandrake 9.2, amd64,10.0, AMD64; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1; Turbolinux Turbolinux Desktop 10.0	A buffer overflow vulnerability exists in the 'ap_resolve_env()' function in 'server/util.c'.due to insufficient validation, which could let a remote malicious user execute arbitrary code. Apache: Upgrade available at: http://www.apache.org/dist/httpd/httpd-2.0.51.tar.gz Patch available at: http://www.apache.org/dist/httpd/patches/apply_to_2.0.50/CAN-2004-0747.patch Gentoo:http://security.gentoo.org/glsa/glsa-200409-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: ftp://updates.redhat.com/enterprise/3WS/en/os/SRPMS/httpd-2.0.46-40.ent.src.rpm SuSE: ftp://ftp.suse.com/pub/suse/ We are not aware of any exploits for this vulnerability. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ TurboLinxux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/ We are not aware of any exploits for this vulnerability.	Apache Web Server Configuration File Buffer Overflow CVE Name: CAN-2004-0747	High	SITIC Vulnerability Advisory, September 15, 2004 US-CERT Vulnerability Note VU#481998, September 17, 2004
Multiple Vendors Cisco VPN 3000 Concentrator 4.0 .x, 4.0, 4.0.1, 4.1 .x; Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Gentoo Linux 1.4 _rc1-rc3, 1.4; MandrakeSoft Corporate Server 2.1, x86_64, Linux Mandrake 9.1, ppc, 9.2, amd64, 10.0, AMD64, MandrakeSoft Multi Network Firewall 8.2; MIT Kerberos 5 1.0, 1.0.6, 1.0.8, 1.1, 1.1.1, 1.2-1.2.8, 1.3 -1.3.4; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3, Fedora Core2, Core1; Sun SEAM 1.0.2	Multiple double-free vulnerabilities exist due to inconsistent memory handling routines in the krb5 library: various double-free errors exist in the KDC (Key Distribution Center) cleanup code and in client libraries, which could let a remote malicious user execute arbitrary code; various double-free errors exist in the 'krb5_rd_cred()' function, which could let a remote malicious user execute arbitrary code; a double-free vulnerability exists in krb524d, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in ASN.1 decoder when handling indefinite length BER encodings, which could let a remote malicious user cause a Denial of Service. MIT Kerberos: http://web.mit.edu/kerberos/advisories/ Cisco: http://www.cisco.com/warp/public/707/cisco-sa-20040831-krb5.shtml Debian: http://security.debian.org/pool/updates/main/k/krb5/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-09.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-21-112908-15-1 Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000860** **OpenPKG: ftp://ftp.openpkg.org/release/** **TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Server/** We are not aware of any exploits for this vulnerability.	Kerberos 5 Double-Free Vulnerabilities CVE Names: CAN-2004-0642, CAN-2004-0643, CAN-2004-0772	Low/High (High if arbitrary code can be executed)	MIT krb5 Security Advisory, MITKRB5-SA-2004-002, August 31, 2004 US-CERT Technical Cyber Security Alert TA04-247A, September 5, 2004 US-CERT Vulnerability Notes, VU#350792, VU#795632, VU#866472, September 3, 2004 **Conectiva Security Advisory, CLSA-2004:860, September 9, 2004** **OpenPKG Security Advisory , OpenPKG-SA-2004.039, September 13, 2004** **Turbolinux Security Advisory TLSA-2004-22, September 15, 2004**
Multiple Vendors Cisco VPN 3000 Concentrator 4.0 .x, 4.0, 4.0.1, 4.1 .x;	A remote Denial of Service vulnerability exists in the ASN.1 decoder when decoding a malformed ASN.1 buffer. MIT Kerberos: http://web.mit.edu/kerberos/advisories/	MIT Kerberos 5 ASN.1 Decoder Remote Denial of Service	Low	MIT krb5 Security Advisory, MITKRB5-SA-2004-002, August 31, 2004

Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Gentoo Linux 1.4 _rc1-rc3, 1.4; MandrakeSoft Corporate Server 2.1, x86_64, Linux Mandrake 9.1, ppc, 9.2, amd64, 10.0, AMD64, MandrakeSoft Multi Network Firewall 8.2; MIT Kerberos 5 1.2.2-1.2.8, 1.3 -1.3.4; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3, Fedora Core2, Core1; Sun Solaris 9.0, 9.0 _x86	Cisco: http://www.cisco.com/warp/public/707/cisco-sa-20040831-krb5.shtml Debian: http://security.debian.org/pool/updates/main/k/krb5/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-09.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57631-1&searchclause= Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000860** **OpenPKG: ftp://ftp.openpkg.org/release/** **TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Server/** We are not aware of any exploits for this vulnerability.	CVE Name: CAN-2004-0644		US-CERT Technical Cyber Security Alert TA04-247A, September 5, 2004 US-CERT Vulnerability Note VU#550464, September 3, 2004 **Conectiva Security Advisory, CLSA-2004:860, September 9, 2004** **OpenPKG Security Advisory , OpenPKG-SA-2004.039, September 13, 2004** **Turbolinux Security Advisory TLSA-2004-22, September 15, 2004**
Multiple Vendors Easy Software Products CUPS 1.1.14-1.1.20; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	A Denial of Service vulnerability exists in 'scheduler/dirsvc.c' due to insufficient validation of UDP datagrams. Update available at: http://www.cups.org/software.php Debian: http://security.debian.org/pool/updates/main/c/cupsys/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/ SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ A Proof of Concept exploit has been published.	CUPS Browsing Denial of Service CVE Name: CAN-2004-0558	Low	SecurityTracker Alert ID, 1011283, September 15, 2004
Multiple Vendors Enlightenment Imlib2 1.0-1.0.5, 1.1, 1.1.1; ImageMagick ImageMagick 5.4.3, 5.4.4 .5, 5.4.8 .2-1.1.0 , 5.5.3 .2-1.2.0, 5.5.6 .0- 2003040, 5.5.7,6.0.2; Imlib Imlib 1.9-1.9.14	Multiple buffer overflow vulnerabilities exist in the Iimlib/Imlib2 libraries when handling malformed bitmap images, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Imlib: http://cvs.sourceforge.net/viewcvs.py/enlightenment/e17/ ImageMagick: http://www.imagemagick.org/www/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200409-12.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Debian: http://security.debian.org/pool/updates/main/i/imagemagick/** **RedHat: http://rhn.redhat.com/errata/RHSA-2004-465.html** **TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/** We are not aware of any exploits for this vulnerability.	IMLib/IMLib2 Multiple BMP Image Decoding Buffer Overflows CVE Names: CAN-2004-0817, CAN-2004-0802	Low/High (High if arbitrary code can be executed)	SecurityFocus, September 1, 2004 Gentoo Linux Security Advisory, GLSA 200409-12, September 8, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:089, September 8, 2004 Fedora Update Notifications, FEDORA-2004-300 &301, September 9, 2004 **Turbolinux Security Advisory, TLSA-2004-27, September 15, 2004** **RedHat Security Advisory, RHSA-2004:465-08, September 15, 2004** **Debian Security Advisories, DSA 547-1 & 548-1, September 16, 2004**
Multiple Vendors Gentoo Linux 1.4; KDE KDE 3.1.3, 3.2, 3.0- 3.0.3, 3.0.5b, 3.0.5, 3.1-3.1.3, 3.1.5, 3.2.1, 3.2.3; MandrakeSoft Linux Mandrake 9.2, amd64, 10.0, AMD64	A vulnerability exists while validating cookie domains, which could let a remote malicious user hijack a target user's session. KDE: ftp://ftp.kde.org/pub/kde/security_patches Gentoo: http://security.gentoo.org/glsa/glsa-200408-23.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora:http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **SuSE: ftp://ftp.suse.com/pub/suse/**	KDE Konqueror Cookie Domain Validation CVE Name: CAN-2004-0746	Medium	KDE Security Advisory, August 23, 2004 Fedora Update Notifications, FEDORA-2004-290 & 291, September 8, 2004 Conectiva Linux Security Announcement, CLA-2004:864, September

	There is no exploit code required.			13, 2004 SUSE Security Announcement, SUSE-SA:2004:026, September 16, 2004

Multiple Vendors
GNU Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha;
GNOME gdk-pixbug 0.22 & prior; GTK GTK+ 2.0.2, 2.0.6, 2.2.1, 2.2.3, 2.2.4;
MandrakeSoft Linux Mandrake 9.2, amd64, 10.0, AMD64;
RedHat Advanced Workstation for the Itanium Processor 2.1, IA64, Desktop 3.0, Enterprise Linux WS 3, WS 2.1 IA64, WS 2.1, ES 3, ES 2.1 IA64, ES 2.1, AS 3, AS 2.1 IA64, AS 2.1, RedHat Fedora Core1&2;
SuSE. Linux 8.1, 8.2, 9.0, x86_64, 9.1, Desktop 1.0, Enterprise Server 9, 8
	Multiple vulnerabilities exist: a vulnerability exists when decoding BMP images, which could let a remote malicious user cause a Denial of Service; a vulnerability exists when decoding XPM images, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and a vulnerability exists when attempting to decode ICO images, which could let a remote malicious user cause a Denial of Service.
	Debian: http://security.debian.org/pool/updates/main/g/gdk-pixbuf/
	Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	Mandrake: http://www.mandrakesecure.net/en/ftp.php
	RedHat: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	SuSE: ftp://ftp.suse.com/pub/suse/
	We are not aware of any exploits for this vulnerability.
		gdk-pixbug BMP, ICO, and XPM Image Processing Errors
		CVE Names: CAN-2004-0753, CAN-2004-0782, CAN-2004-0783, CAN-2004-0788
			Low/High
			(High if arbitrary code can be executed)
				SecurityTracker Alert ID, 1011285, September 17, 2004

Multiple Vendors LinuxPrinting.org Foomatic-Filters 3.03.0.2, 3.1; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	A vulnerability exists in the foomatic-rip print filter due to insufficient validation of command-lines and environment variables, which could let a remote malicious user execute arbitrary commands. Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ We are not aware of any exploits for this vulnerability.	LinuxPrinting.org Foomatic-Filter Arbitrary Code Execution CVE Name: CAN-2004-0801	High	Secunia Advisory, SA12557, September 16, 2004
Multiple Vendors Luke Mewburn lukemftp 1.5, TNFTPD 20031217; NetBSD Current, 1.3-1.3.3, 1.4 x86, 1.4, SPARC, arm32, Alpha, 1.4.1 x86, 1.4.1, SPARC, sh3, arm32, Alpha, 1.4.2 x86, 1,4.2, SPARC, arm32, Alpha, 1.4.3, 1.5 x86, 1.5, sh3, 1.5.1-1.5.3, 1.6, beta, 1.6-1.6.2, 2.0	Several vulnerabilities exist in the out-of-band signal handling code due to race condition errors, which could let a remote malicious user obtain superuser privileges. Luke Mewburn Upgrade: ftp://ftp.netbsd.org/pub/NetBSD/misc/tnftp/tnftpd-20040810.tar.gz Apple: http://wsidecar.apple.com/cgi-bin/ **Gentoo: http://security.gentoo.org/glsa/glsa-200409-19.xml** We are not aware of any exploits for this vulnerability.	TNFTPD Multiple Signal Handler Remote Privilege Escalation CVE Name: CAN-2004-0794	High	NetBSD Security Advisory 2004-009, August 17, 2004 Apple Security Update, APPLE-SA-2004-09-07, September 7, 2004 **Gentoo Linux Security Advisory, GLSA 200409-19, September 16, 2004**

Multiple Vendors
OpenBSD 3.4, 3.5;
SuSE Linux 8.1, 8.2, 9.0, x86_64, 9.1, Linux Enterprise Server 9, 8;
X.org X11R6 6.7.0, 6.8;
XFree86 X11R6 3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1, Errata, 4.3.0
	Multiple vulnerabilities exist: a stack overflow exists in 'xpmParseColors()' in 'parse.c' when a specially crafted XPMv1 and XPMv2/3 file is submitted, which could let a remote malicious user execute arbitrary code; a stack overflow vulnerability exists in the 'ParseAndPutPixels()' function in -create.c' when reading pixel values, which could let a remote malicious user execute arbitrary code; and an integer overflow vulnerability exists in the colorTable allocation in 'xpmParseColors()' in 'parse.c,' which could let a remote malicious user execute arbitrary code.
	Debian: http://security.debian.org/pool/updates/main/i/imlib/
	Mandrake: http://www.mandrakesecure.net/en/ftp.php
	OpenBSD: ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/
	SuSE: ftp://ftp.suse.com/pub/suse/
	X.org: http://x.org/X11R6.8.1/
	Proofs of Concept exploits have been published.
		LibXpm Image Decoding Multiple Remote Buffer Overflow
		CVE Names: CAN-2004-0687, CAN-2004-0688
			High	X.Org Foundation Security Advisory, September 16, 2004

Multiple Vendors SuSE Linux 8.1, 8.2, 9.0, x86_64, 9.1,	A remote Denial of Service vulnerability exists in the smbd and nmbd daemons. Samba: http://us3.samba.org/samba/ftp/samba-3.0.7.tar.gz	Samba-VScan Remote Denial of Service	Low	SUSE Security Announcement, SA:2004:034, September 17, 2004

Linux Enterprise Server 9, 8; Samba 3.0-3.0.6	SuSE: ftp://ftp.suse.com/pub/suse/ We are not aware of any exploits for this vulnerability.			
OpenOffice OpenOffice 1.1.2, Sun StarOffice 7.0	A vulnerability exists in the '/tmp' folder due to insecure permissions, which could let a malicious user obtain sensitive information. Upgrades available at: http://sunsolve.sun.com/search/ **RedHat: http://rhn.redhat.com/errata/RHSA-2004-446.html** There is no exploit code required.	OpenOffice/ StarOffice Insure Temporary File Permissions CVE Name: CAN-2004-0752	Medium	Secunia Advisory, SA12302, September 13, 2004 **RedHat Security Bulletin, RHSA-2004:446-08, September 15, 2004**
Peter D. Gray SUS 2.0, 2.0.1	A format string vulnerability exists in the 'log()' function due to insufficient sanitization, which could let a malicious user obtain root access. Upgrades available at: http://pdg.uow.edu.au/sus/sus-2.0.6.tar.Z Gentoo: http://security.gentoo.org/glsa/glsa-200409-17.xml A Proof of Concept exploit has been published.	SUS Format String	High	LSS Security Advisories, September 14, 2004 Gentoo Linux Security Advisory, GLSA 200409-17, September 14, 2004
PHP Group Debian Slackware Fedora pp 4.3.7 and prior	Updates to fix multiple vulnerabilities with php4 which could allow remote code execution. Debian: Update to Debian GNU/Linux 3.0 alias woody at http://www.debian.org/releases/stable/ Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.406480 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ **TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Server/** We are not aware of any exploits for this vulnerability.	PHP 'memory_limit' and strip_tags() Remote Vulnerabilities CVE Names: CAN-2004-0594, CAN-2004-0595	High	Secunia, SA12113 and SA12116, July 21, 2004 Debian, Slackware, and Fedora Security Advisories **Turbolinux Security Advisory TLSA-2004-23, September 15, 2004**
Samba Samba 2.2.11, 3.0.6; **SuSE Linux 8.1, 8.2, 9.0, x86_64, 9.1, Enterprise Server 9, 8**	A remote Denial of Service vulnerability exists due to the way print change notify requests are processed. Trustix: http://http.trustix.org/pub/trustix/updates/ **Gentoo: http://security.gentoo.org/glsa/glsa-200409-14.xml** **Samba: http://us4.samba.org/samba/ftp/samba-2.2.11.tar.gz** **SuSE: ftp://ftp.suse.com/pub/suse/** **TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32** We are not aware of any exploits for this vulnerability.	Samba Remote Print Change Notify Remote Denial of Service CVE Name: CAN-2004-0829	Low	Trustix Secure Linux Security Advisory, TSL-2004-0043, August 26, 2004 **Gentoo Linux Security Advisory, [ERRATA UPDATE] GLSA 200409-14:02, September 9, 2004** **Turbolinux Security Advisory, TLSA-2004-25, September 15, 2004** **SUSE Security Announcement, SUSE-SA:2004:034, September 17, 2004**
Samba.org Samba version 3.0 - 3.0.6	Several vulnerabilities exist: a remote Denial of Service vulnerability exists in the 'process_logon_packet()' function due to insufficient validation of 'SAM_UAS_CHANGE' request packets; and a remote Denial of Service vulnerability exists when a malicious user submits a malformed packet to a target 'smbd' server. Updates available at: http://samba.org/samba/download/ **Gentoo: http://security.gentoo.org/glsa/glsa-200409-16.xml** **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **OpenPKG: ftp://ftp.openpkg.org/release/2.1/UPD/** **SuSE: ftp://ftp.suse.com/pub/suse/** **Trustix: http://http.trustix.org/pub/trustix/updates/** We are not aware of any exploits for this vulnerability.	Samba Remote Denials of Service CVE Names: CAN-2004-0807, CAN-2004-0808	Low	Securiteam, September 14, 2004 **Gentoo Linux Security Advisory, GLSA 200409-16, September 13, 2004** **Mandrakelinux Security Update Advisory, MDKSA-2004:092, September 13, 2004** **Trustix Secure Linux Bugfix Advisory, TSL-2004-0046, September 14, 2004** **OpenPKG Security Advisory, OpenPKG-SA-2004.040, September 15, 2004** **SUSE Security Announcement, SUSE-SA:2004:034, September 17, 2004**
SnipSnap SnipSnap 0.5.2 a	A vulnerability exists in the 'referer' parameter due to the way POST requests are handled, which could let a remote malicious user execute arbitrary code.	SnipSnap HTTP Response Splitting	Medium	Bugtraq, September, 14, 2004

	Upgrade available at: http://snipsnap.org/space/snipsnap-DOWNLOAD Gentoo: http://security.gentoo.org/glsa/glsa-200409-23.xml A Proof of Concept exploit has been published.			Gentoo Linux Security Advisory, GLSA 200409-23, September 17, 2004
SpamAssassin.org SpamAssassin prior to 2.64	A Denial of Service vulnerability exists in SpamAssassin. A a remote user can send an e-mail message with specially crafted headers to cause a Denial of Service attack against the SpamAssassin service. Update to version (2.64), available at: http://old.spamassassin.org/released/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **OpenPKG: ftp://ftp.openpkg.org/release/** We are not aware of any exploits for this vulnerability.	SpamAssassin Remote Denial of Service	Low	SecurityTracker: 1010903, August 10, 2004 Mandrake Security Advisory, MDKSA-2004:084, August 19, 2004 **OpenPKG Security Advisory, OpenPKG-SA-2004.041, September 15, 2004**
Squid-cache.org Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 STABLE5, 2.4, STABLE7, 2.5 STABLE1-STABLE6, Squid Web Proxy Cache 3.0 PRE1-PRE3	A remote Denial of Service vulnerability exists in 'lib/ntlmauth.c' due to insufficient validation of negative values in the 'function "ntlm_fetch_string()' function. Patches available at: http://www1.uk.squid-cache.org/squid/Versions/v2/2.5/bugs/squid-2.5.STABLE6-ntlm_fetch_string.patch Gentoo: http://security.gentoo.org/glsa/glsa-200409-04.xml **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **Trustix: http://http.trustix.org/pub/trustix/updates/** We are not aware of any exploits for this vulnerability.	Squid Proxy NTLM Authentication Remote Denial of Service CVE Name: CAN-2004-0832	Low	Secunia Advisory, SA12444, September 3, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:093, September 15, 2004** **Trustix Secure Linux Security Advisory, TSLSA-2004-0047, September 16, 2004**
Todd Miller Sudo 1.6.8	A vulnerability exists due to insufficient validation of symbolic links when sudoedit ("sudo -u" option) copies temporary files, which could let a malicious user access the contents of arbitrary files with superuser privileges. Upgrade available at: ftp://ftp.sudo.ws/pub/sudo/sudo-1.6.8p1.tar.gz There is no exploit code required; however, a Proof of Concept exploit script has been published.	Sudo Information Disclosure	High	Secunia Advisory, SA12596, September 20, 2004
VBulletin VBulletin 3.0, Gamma, beta 2-beta7, 3.0.1-3.0.3	A vulnerability exists in the 'x_invoice_num' parameter due to insufficient validation, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	vBulletin SQL Injection	High	Securiteam, September 14, 2004
xinehq.de xine 0.5.2 - 0.5.x; 0.9.x; 1-alpha.x; 1-beta.x; 1-rc - 1-rc5	Multiple vulnerabilities exist: a buffer overflow in the DVD subpicture component, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the VideoCD functionality when reading ISO disk labels, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists when handling text subtitles, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/xine/xine-lib-1-rc6a.tar.gz?download We are not aware of any exploits for this vulnerability.	Xine-lib Multiple Buffer Overflows	High	Secunia Advisory, SA12602 September 20, 2004

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Business Objects InfoView 5.1.4-5.1.8, WebIntelligence 2.7-2.7.4	Two vulnerabilities exist: a vulnerability exists because some security checks are performed on the client-side and not on the server-side, which could let an authenticated remote malicious user delete arbitrary documents; and a Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied input when uploading documents, which could let a remote malicious user execute arbitrary HTML and script code. The vendor has released patches dealing with this issue. Users are recommended to contact the vendor for patch and update availability. There is no exploit code required.	WebIntelligence Access Control Bypass & Cross-Site Scripting CVE Names: CAN-2004-0533, CAN-2004-0534	Medium/ High (High if arbitrary code can be executed)	Corsaire Security Advisory, September 17, 2004
Hewlett Packard Company Web Jetadmin 7.5, 7.5.2456	An unspecified vulnerability exists which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.hp.com/go/webjetadmin We are not aware of any exploits for this vulnerability.	HP Web Jetadmin Unspecified Arbitrary Command Execution	High	HP Security Advisory, SSRT4739, September 15, 2004
Inkra Networks Corporation	A remote Denial of Service vulnerability exists due to insufficient validation of IP options.	Inkra 1504GX Remote Denial of Service	Low	Secunia Advisory, SA12538,

1504GX VSM 2.1.4.b003	No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploit has been published.			September 17, 2004
Matt Smith ReMOSitory	An input validation vulnerability exists in the ReMOSitory add-on for Mambo Open Server due to insufficient validation, which could let a remote malicious user execute arbitrary code. The vendor indicates that ReMOSitory is no longer supported; however, Arthur Konze from mamboportal.com has provided a patch, available at: http://www.mamboportal.com/uploadfiles/remository_fix.zip A Proof of Concept exploit has been published.	ReMOSitory SQL Injection	High	Bugtraq, September 18, 2004
Mozill.org Mozilla 0.x, 1.0-1.7.x, Firefox 0.x, Thunderbird 0.x; Netscape Navigator 7.0, 7.0.2, 7.1, 7.2	Multiple vulnerabilities exist: buffer overflow vulnerabilities exist in 'nsMsgCompUtils.cpp' when a specially crafted e-mail is forwarded, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to insufficient restrictions on script generated events, which could let a remote malicious user obtain sensitive information; a buffer overflow vulnerability exists in the 'nsVCardObj.cpp' file due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in 'nsPop3Protocol.cpp' due to boundary errors, which could let a remote malicious user execute arbitrary code; a heap overflow vulnerability exists when handling non-ASCII characters in URLs, which could let a remote malicious user execute arbitrary code; multiple integer overflow vulnerabilities exist in the image parsing routines due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code; a cross-domain scripting vulnerability exists because URI links dragged from one browser window and dropped into another browser window will bypass same-origin policy security checks, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because unsafe scripting operations are permitted, which could let a remote malicious user manipulate information displayed in the security dialog. Updates available at: http://www.mozilla.org/ Proofs of Concept exploits have been published.	Mozilla Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Technical Cyber Security Alert TA04-261A, September 17, 2004 US-CERT Vulnerability Notes VU#414240, VU#847200, VU#808216, VU#125776, VU#327560, VU#651928, VU#460528, VU#113192, September 17, 2004
Multiple Vendors Microsoft Internet Explorer 6.0, SP1&SP2; Mozilla Firefox 0.9.2	A vulnerability exists while validating cookie domains, which could let a remote malicious user hijack a target user's session. No workaround or patch available at time of publishing. There is no exploit code required.	Multiple Browser Cookie Domain Validation CVE Names: CAN-2004-0866, CAN-2004-0867	Medium	Westpoint Security Advisory, September 15, 2004
Multiple Vendors HP HP-UX B.11.23, 11.11, 11.00; Mozilla Network Security Services (NSS) 3.2, 3.2.1, 3.3-3.3.2, 3.4-3.4.2, 3.5, 3.6, 3.6.1, 3.7-3.7.3, 3.7.5, 3.7.7, 3.8, 3.9; Netscape Certificate Server 1.0 P1, 4.2, Directory Server 1.3, P1&P5, 3.12, 4.1, 4.11-.4.13, Enterprise Server 2.0 a, 2.0, 2.0.1 C, 3.0 L, 3.0, 3.0.1 B, 3.0.1, 3.1, 3.2, 3.5, 3.6, SP1-SP3, 3.51, 4.0, 4.1, SP3-SP8, Enterprise Server for NetWare 4/5 3.0.7 a, 4/5 4.1.1, 4/5 5.0, Enterprise Server for Solaris 3.5, 3.6, Netscape Personalization Engine; Sun ONE Application Server 6.0, SP1-SP4, 6.5, SP1 MU1&MU2, 6.5 SP1, 6.5 MU1-MU3, 7.0 UR2 Upgrade Standard, 7.0 UR2 Upgrade Platform, Standard Edition, Platform Edition, 7.0 UR1 Standard Edition, Platform Edition, 7.0 Standard Edition, Platform Edition, Certificate Server 4.1, Directory Server 4.16, SP1, 5.0, SP1&SP2, 5.1 x86 SP3 x86, 5.1, SP1-SP3, 5.2, Web Server 4.1, SP1-SP14, 6.0, SP1-SP7, 6.1	A buffer overflow vulnerability exists in the Netscape Network Security Services (NSS) library suite due to insufficient boundary checks, which could let a remote malicious user which may result in remote execute arbitrary code. Mozilla:/ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_9_2_RTM/ **Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57643-1&searchclause=security** We are not aware of any exploits for this vulnerability.	NSS Buffer Overflow	High	Internet Security Systems Advisory, August 23, 2004 **Sun(sm) Alert Notification, 57643, September 16, 2004**
myserverproject.net MyServer 0.7	A Directory Traversal vulnerability exists due to an input validation error, which could let a remote malicious user obtain sensitive information.	MyServer Directory Traversal	Medium	securiteinfo.com advisory, September 15,

	Update available at: http://sourceforge.net/projects/myserverweb/ There is no exploit code required; however, a Proof of Concept exploit has been published.			2004
PHP Group PHP 5.0 - 5.0.1	A vulnerability exists in the 'phpinfo()' function, which could let a remote malicious user obtain sensitive information. Update available at: http://chora.php.net/php-src/main/php_variables.c A Proof of Concept exploit has been published.	PHP 'phpinfo()' Function Information Disclosure	Medium	SecurityTracker Alert ID, 1011279, September 15, 2004
PHPGroupWare PHPGroupWare 0.9.12-0.9.16	A Cross-Site Scripting vulnerability exists in 'transforms.php' due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at: http://downloads.phpgroupware.org/files/0.9.16-release/phpgroupware-0.9.16.003.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200409-22.xml There is no exploit code required.	PHPGroupWare Cross-Site Scripting	High	SecurityTracker Alert ID, 1011339, September 17, 2004
SMC SMC7004VWBR 1.21 a, 1.22, 1.23, SMC7008ABR 1.32	A vulnerability exists which due to the way users are validated in the web administration software, which could let a remote malicious user obtain administrative access. No workaround or patch available at time of publishing. There is no exploit code required.	SMC7004VWBR & SMC7008ABR Authentication Bypass	High	Secunia Advisory, SA12601, September 20, 2004
YaBBSE.org YaBB 1 Gold Release, SP 1.3.1, SP 1.3, SP 1.2, SP 1, YaBB 1.40, 1.41, 9.1.2000, 9.11.2000	Several vulnerabilities exist: a vulnerability exists due to a failure to properly validate access to administrative commands, which could let a remote malicious user execute arbitrary commands; and a Cross-Site Scripting vulnerability exists in the 'YaBB.pl' script, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	YaBB Administrator Command Execution & Cross-Site Scripting	High	Bugtraq, September 16, 2004
ZyXEL Communications Corp. Prestige 681	An information disclosure vulnerability exists in ARP requests, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	ZyXEL P681 ARP Request Information Disclosure	Medium	Bugtraq, September 13, 2004

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Exploit (Reverse Chronological Order)	Script or Exploit Name	Workaround or Patch Available	Description
September 21, 2004	advisory-05-glFTPd.txt	No	Proof of concept exploit for the local stack overflow vulnerability in the dupescan binary from glFTPd versions 2.00RC3 and below.
September 21, 2004	ettercap-NG-0.7.1.tar.gz	N/A	Ettercap NG is a network sniffer/interceptor/logger for switched LANs. It uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
September 21, 2004	mambo45.jose.txt	Yes	Mambo versions 4.5 and below are susceptible to cross site scripting and remote command execution flaws.
September 21, 2004	mambo451.txt	Yes	Proof of concept exploit for Mambo versions 4.5.1 and below SQL injection vulnerability.
September 21, 2004	pigeonx.zip	Yes	Remote denial of service exploit for Pigeon versions 3.02.0143 and below.
September 21, 2004	rsynxOSX.txt	Yes	Proof of concept exploit for RsyncX version 2.1, the frontend for rsync on OS X, arbitrary program execution vulnerability.
September 21, 2004	sudoedit.txt	Yes	Proof of concept exploit for sudo version 1.6.8p1 that makes use of a flaw in sudoedit.
September 18, 2004	sudo-exploit.c	Yes	Proof of Concept exploit for the Sudo Information Disclosure vulnerability.
September 17, 2004	CRASH-TEST.zip crash-netscape.jpg jpegcompoc.zip	Yes	Proof of concept exploit for the Microsoft (Graphics Device Interface) GDI+ JPEG handler integer underflow vulnerability.
September 17, 2004	jpegcompoc.zip	Yes	Proof of concept exploit for the JPEG buffer overrun vulnerability in Windows XP.
September 17, 2004	lovethisgame.html	No	Proof of concept exploit for a file inclusion vulnerability in PerlDesk 1.x due to insufficient input validation.
September 17, 2004	None	No	Example exploit for the DNS4Me denial of service and cross-site scripting vulnerabilities.
September 17, 2004	None	No	Example exploit for the cross-site scripting vulnerability in the YaBB forum 'YaBB.pl' script.
September 17, 2004	None	No	Proof of concept exploit for the Google Toolbar HTML injection vulnerability. It is reported that the Google Toolbar 'ABOUT.HTML' page allows the injection of HTML and JavaScript code.
September 17, 2004	None	No	Example exploit for the YaBB administrator command execution vulnerability.
September 17, 2004	None	Yes	Proof of concept exploit for the Mozilla and Firefox cross-domain scripting vulnerability.
September 17, 2004	None	Yes	Proof of concept exploit for the SnipSnap HTTP response splitting vulnerability.

September 16, 2004	None	Yes	Proof of concept exploit for the Snitz Forums HTTP response splitting vulnerability.
September 16, 2004	Tx.exe	Yes	A small universal Windows backdoor for all versions of Windows NT/2K/XP/2003 with any service pack.
September 15, 2004	bbsEMarket.txt	Yes	Proof of concept exploit for BBS E-Market Professional path disclosure, file download, file disclosure, user authentication bypass, and php source injection vulnerabilities. BBS E-Market patch level bf_130, version 1.3.0, and below is affected.
September 15, 2004	cdr-exp.sh cdrecord-suidshell.sh readcd-exp.sh	Yes	CDRTools is reportedly vulnerable to an RSH environment variable privilege escalation vulnerability. This issue is due to a failure of the application to properly implement security controls when executing an application specified by the RSH environment variable.
September 15, 2004	challenges.tgz	N/A	This package contains example vulnerable C programs. There are examples of buffer overflows (stack and heap) and format string vulnerabilities. All examples are exploitable with a standard linux/x86 environment.
September 15, 2004	fwknop-0.4.1.tar.gz	N/A	fwknop is a flexible port knocking implementation that is based around iptables. Both shared knock sequences and encrypted knock sequences are supported.
September 15, 2004	myServer07.txt	Yes	myServer version 0.7 is susceptible to a simple directory traversal attack.
September 15, 2004	netw-ib-ox-ag-5.24.0.tgz	N/A	Netwox is a utility that supports various protocols (DNS, FTP, HTTP, NNTP, SMTP, SNMP) and performs low level functions like sniffing, spoofing traffic, and playing client/server roles. Both Windows and Unix versions are included.
September 15, 2004	None	Yes	Proof of concept vulnerability for the vulnerability in the Mozilla 'enablePrivilege' method.
September 15, 2004	None	Yes	Proof of concept exploit for the vulnerability in Mozilla and Firefox browsers that could permit a remote site to gain access to contents of the client user's clipboard.
September 15, 2004	pizzaicmp.c	N/A	ICMP-based triggered Linux kernel module that executes a local binary upon successful use.
September 15, 2004	Rx.exe	Yes	A small universal Windows reverse shell for all versions of Windows NT/2K/XP/2003 with any service pack.
September 14, 2004	getinternet.txt	No	Proof of concept exploit for getInternet SQL injection and remote command execution vulnerabilities
September 14, 2004	getintranet.txt	No	Proof of concept exploit for getIntranet 2.x cross site scripting, SQL injection, script insertion, and multiple other attacks vulnerabilities.
September 14, 2004	LSS-2004-09-01.html	Yes	Proof of concept exploit for the format string vulnerability in SuS logging function.
September 14, 2004	regulus.htm	No	Proof of concept exploit for various vulnerabilities exist in Regulus 2.x that allow for an attacker to gain access to sensitive information and to bypass certain security restrictions.
September 13, 2004	None	Yes	Proof of concept exploit for Webmin / Usermin command execution vulnerability when rendering HTML email messages. This issue is reported to affect Usermin versions 1.080 and prior.
September 13, 2004	None	Yes	Proof of concept exploit for the Pingtel Xpressa handset remote denial of service vulnerability.
September 13, 2004	None	No	Proof of concept exploit for the QNX Photon MicroGUI buffer overflow vulnerabilities in MicroGUI utilities.
September 11, 2004	None	No	Proof of concept vulnerability for the Serv-U FTP Server denial of service vulnerability.

[back to top]

Trends

- Several vulnerabilities exist in the Mozilla web browser and derived products, the most serious of which could allow a remote attacker to execute arbitrary code on an affected system. Mozilla has released versions of the affected software that contain patches for these issues: Mozilla 1.7.3, Firefox Preview Release, Thunderbird 0.8. Users are strongly encouraged to upgrade to one of these versions: www.mozilla.org. For more information, see US-CERT Technical Cyber Security Alert TA04-261A: Multiple vulnerabilities in Mozilla products. Available at: http://www.uscert.gov/cas/techalerts/TA04-261A.html
- The volume of worms and viruses is increasing, but the rate of successful attacks has dropped, according to a new report from Symantec. The antivirus company's biannual Internet Security Threat Report found that 4,496 new Windows viruses and worms were released between January and June, up more than 4.5 times from same period last year. But overall the daily volume of actual attacks decreased in the first six months of 2004. Alfred Huger, a senior director at Symantec's Security Response team said malicious code writers were increasingly going to spammers to sell them access to the computers that they hack, or break into. Spammers, after paying the hackers, then flood those hacked computers with unsolicited messages or spam. Symantec also said it expects more viruses and worms in the future to be written to attack systems that run on the Linux operating system and hand-held devices as they become more widely used. The report also noted that the rate at which personal computers are being hijacked by hackers rocketed in the first half of 2004. An average of 30,000 computers per day were turned into enslaved “zombies”, compared with just 2000 per day in 2003. Report: http://enterprisesecurity.symantec.com/content.cfm?articleid =1539 (CNET News.com, September 20, 2004)

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Zafi-B	Win32 Worm	Stable	June 2004
3	Netsky-Z	Win32 Worm	Stable	April 2004
4	Netsky-D	Win32 Worm	Stable	March 2004
5	Netsky-B	Win32 Worm	Stable	February 2004
6	Mydoom.m	Win32 Worm	Increase	July 2004
7	Mydoom.q	Win32 Worm	Slight Decrease	August 2004

8	Bagle-AA	Win32 Worm	Slight Decrease	April 2004
9	Netsky-Q	Win32 Worm	Stable	March 2004
10	MyDoom-O	Win32 Worm	Decrease	July 2004

Top Ten Table Updated September 17, 2004

Viruses or Trojans Considered to be a High Level of Threat

- Troj/IBank-A: Sophos is warning computer users about a Trojan horse that helps hackers break into the bank accounts of customers of an Australian bank. The Troj/IBank-A Trojan horse is designed to steal information from Internet customers of the National Australia Bank, which could allow hackers to break into accounts and steal substantial amounts of money. Although this particular Trojan horses only targets users of an Australian bank, Sophos warns that others have been seen which affect banking customers in other parts of the world.

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Nemog.D		Trojan
Backdoor.Sdbot.AA		Trojan
Backdoor.Sdbot.AB		Trojan
BackDoor-CIM		Trojan
Bagle.BA	W32/Bagle.BA.worm	Win32 Worm
Downloader-OT		Trojan
Downloader-PU		Trojan
E2Give		Trojan
Fightrub.A	W32/Fightrub.A.worm W32/Fightrub@MM	Win32 Worm
Hacktool.IPCscan		Trojan
Java/Binny.A		Trojan
JS/Zerolin.eml		Trojan
Mitglieder.cc	TrojanProxy.Win32.Mitglieder.cc	Trojan
MyDoom.AB	I-Worm.Mydoom.y W32.Mydoom.AB@mm W32/Mydoom.AB@mm Win32.Mydoom.AA Win32/Mydoom.AA.Worm	Win32 Worm
Troj/IBank-A	PWSteal.Ibank	Trojan: Password Stealer
Trojan.Anits		Trojan
VBS.Vabi@mm		Visual Basic Worm
W32.Mexer.E@mm		Win32 Worm
W32.Sndog@mm		Win32 VB Worm
W32.Spybot.CYM		Win32 Worm
W32/Fightrub@MM		Win32 Worm
W32/Forbot-AE	Backdoor.Win32.Wootbot.gen W32/Gaobot.worm.gen.f	Win32 Worm
W32/Forbot-Gen		Win32 Worm
W32/Forbot-W		Win32 Worm
W32/Mydoom.ab@MM		Win32 Worm
W32/Mydoom-Y	Win32.Evaman.D@mm W32/Evaman.e@MM I-Worm.Mydoom.w	Win32 Worm
W32/MyDoom-Z	I-Worm.Mydoom.y	Win32 Worm
W32/Myfip-A	W32/Myfip.worm	Win32 Worm
W32/Pahac@MM		Win32 Worm
W32/Rbot-JR	Backdoor.Rbot.gen WORM_RBOT.LU	Win32 Worm
W32/Rbot-KZ	Backdoor.Rbot.gen	Win32 Worm
W32/Sasser-G	Worm.Win32.Sasser.g	Win32 Worm
W32/Sdbot-PG	BKDR_SDBOT.GEN	Win32 Worm
W32/Sdbot-PI	Trojan.Win32.Pakes	Win32 Worm
W32/Sdbot-PJ	Backdoor.SdBot.gen	Win32 Worm
W32/Sdbot-PK		Win32 Worm
W32/Squirrel-A		Win32 Worm
Win32.Bagle.AL	I-Worm.Bagle.ap W32.Beagle.AQ@mm W32/Bagle.aw Win32/Bagle.AW.Worm	Win32 Worm
Win32.Daqa.D	BackDoor-BDI Backdoor.Win32.Agent.co Win32.Daqa.D Win32/Agent.CO.Trojan	Trojan

Win32.Evaman.D	Evaman.D I-Worm.MyDoom.gen W32.Evaman.C@mm W32/Evaman.D.worm W32/Evaman.d@MM	Win32 Worm
Win32.Evaman.D	Evaman.D I-Worm.MyDoom.gen W32.Evaman.C@mm W32/Evaman.D.worm W32/Evaman.d@MM	Win32 Worm
Win32.Evaman.E	I-Worm.Mydoom.w MyDoom.AC W32/Evaman.e@MM W32/Mydoom.AC@mm Win32/Evaman.E.Worm	Win32 Worm
Win32.Mydoom.AA	I-Worm.Mydoom.y W32/Mydoom.ab@MM	Win32 Worm
Win32.Remadmin.A		Win32 Worm
Win32.Slinbot.LY	Backdoor.SdBot.gen IRC/SdBot.BXT W32/Sdbot.worm.gen.q Win32/Slinbot.LY.Worm	Win32 Worm
Win32.Sokeven.D	Win32/Sokeven.D.Trojan	Win32 Worm
WM97/Bablas-FA		MS Word Macro Virus
WORM_EVAMAN.C		Win32 Worm
WORM_MEXER.E		Win32 Worm
WORM_MYDOOM.U	W32/Mydoom.u@MM	Win32 Worm
WORM_SDBOT.VQ		Win32 Worm

[back to top]

Last updated